LOGON BANNER POLICY 0935

(April 2015)

The California Department of Forestry and Fire Protection (CAL FIRE) Information Security Office, in collaboration with Information Technology Services, is responsible for safeguarding and maintaining the integrity of its information and electronic assets.

In order to create a uniform policy for the California Natural Resources Agency (CNRA) and its organizational entities, ISO 1.0 was issued to all organizational entities requiring the use of a logon banner. A logon banner refers to a display of electronic messages that provide notice of legal rights and responsibilities for proper use to the user of a computer network and systems.

The logon banner gives notice to unauthorized users of serious consequences for attempting entry into a government-owned information system and informs authorized users of their rights, responsibilities, and the consequences of misuse of the information they are about to access.

REFERENCE(S) 0935.1

(April 2015)

CNRA Information Security Policy ISO 1.0
State Administrative Manual Section 5300 et seq.
California Penal Code Section 502
California Civil Code Section 1798 et seq.

GENERAL PROVISION 0935.2

(April 2015)

This policy applies to employees and to any and all other persons authorized to access CAL FIRE information assets, regardless of classification or job assignment, including, but not limited to, business partners, contractors, sub-contractors, vendors, and/or volunteer staff.

The logon banner safeguards electronic assets by providing the following:

1. The consequences of unauthorized access or misuse.

2. A warning to unauthorized individuals that they are attempting to access a government computer resource and that their actions will be monitored.

3. A basis for the prosecution of attackers that have compromised the system.

4. A specific warning to potential attackers that they are attempting to access State owned government computers and ensures that they can be prosecuted under California Penal Code Section 502.

5. A reminder to authorized users that network systems are assets of the Natural Resources Agency and Agency entities.

6. A reminder to authorized users of the systems that they can have no expectation of privacy and that use of any system is subject to monitoring to ensure proper use and identify misuse.

7. The purposes and/or justifications of any monitoring/search, and what may be done with the outcome of any monitoring/search.

   It is the Department's position that clicking acceptance of the restrictions identified in the logon banner constitutes the user's informed consent to monitoring and serves as an acknowledgement that the user has no reasonable expectation of privacy.

PROCEDURES 0935.3

(April 2015)

The logon banner requires users to acknowledge the logon banner prior to being allowed access to the networks or systems. The logon banner shall read as follows:

"WARNING! This government computer system is the property of the California Department of Forestry and Fire Protection (CAL FIRE) and may only be accessed by authorized users. Unauthorized access, use, disruption, modification, or destruction of this system is strictly prohibited and may be subject to criminal prosecution and/or adverse action. CAL FIRE may monitor any activity or communications on the system and retrieve any information stored within the system. By accessing and using this system, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users can have no expectation of privacy as to any communication on or information created, maintained, and stored within the system, including information stored centrally, locally on a disk drive, or on removable electronic storage media. In addition to any other available remedies, the penalties for unauthorized access or use may include criminal and/or civil action under the California Information Privacy Act (Financial Code Section 1798.53) and Penal Code Section 502."

Logon banners must be implemented for all access points, applications, networks and systems including, but not limited to:

- External and Legacy systems access
- Mainframe and server applications
- System-administration access (e.g., servers, network devices, email, web access and virtual private network access servers)

Access points are defined as enterprise network, remote access, system-administration, applications, and data system specific access. This includes, but is not limited to, server access achieved with handheld devices, smart-phones, laptops, and remote log-in from home computers. Access points that do not comply with the use of logon banners shall be reported to the CAL FIRE Information Security Office.

The logon banner must be incorporated when initiating projects, establishing new infrastructure platforms, performing business applications updates, and in the change control process.

(see next section)

(see HB Table of Contents)

(see Forms or Forms Samples)